Timothy L. Alger, Bar No. 160303
TAlger@perkinscoie.com
Julie E. Schwartz, Bar No. 260624
JSchwartz@perkinscoie.com
PERKINS COIE LLP
3150 Porter Drive
Palo Alto, CA 94304-1212
Telephone: 650.838.4300
Facsimile: 650.838.4350

Amanda J. Beane (*pro hac vice*)
ABeane@perkinscoie.com
PERKINS COIE LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101-3099
Telephone: 206.359.8000
Facsimile: 206.359.9000

Attorneys for Defendant
Twitter, Inc.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

MARC OPPERMAN, et al.,

Plaintiffs,

v.

PATH, INC., et al.,

Defendants.

Case No. 13-cv-00453-JST

TWITTER, INC.'S MOTION TO DISMISS SECOND CONSOLIDATED AMENDED COMPLAINT

DATE: December 2, 2014
TIME: 2:00 p.m.
COURTROOM: 9
JUDGE: Hon. Jon S. Tigar

THIS DOCUMENT RELATES TO CASES:

Opperman v. Path, Inc., No. 13-cv-00453-JST
Hernandez v. Path, Inc., No. 12-cv-1515-JST
Pirozzi v. Apple, Inc., No. 12-cv-1529-JST

NOTICE OF MOTION AND MOTION TO DISMISS
SECOND CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE that on December 2, 2014 at 2:00 p.m., or at such other time convenient for the Court, in the courtroom of the Honorable Jon S. Tigar, located at 450 Golden Gate Avenue, San Francisco, California, Defendant Twitter, Inc. ("Twitter") will and hereby does move for an order dismissing Plaintiffs' Second Consolidated Amended Complaint under Rules 12(b)(1) and 12(b)(6) of the Federal Rules of Civil Procedure and Article III of the United States Constitution.

This Motion is based on this Notice of Motion and Motion, the Memorandum of Points and Authorities, the Declaration of Sung Hu Kim and exhibits thereto, the Court's files in this action, the arguments of counsel, and any other matter that the Court may properly consider.

DATED: August 21, 2014

PERKINS COIE LLP

By: */s/ Timothy L. Alger*
Timothy L. Alger

Attorneys for Defendant
Twitter, Inc.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

STATUTES

RULES

OTHER AUTHORITIES

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

The Second Consolidated Amended Complaint ("SCAC") now before the Court is the *fifth* attempt by Plaintiffs[1] to plead a viable claim for relief against Defendant Twitter, Inc. ("Twitter"). Plaintiffs assert that they were harmed by Twitter's "Follow Your Friends" feature – which allows users to quickly and efficiently determine whether their acquaintances are also using Twitter – because the feature allegedly copied address book contacts from Plaintiffs' mobile devices onto Twitter's computer servers.

The Court previously dismissed all but one claim against Twitter in Plaintiffs' Consolidated Amended Complaint ("CAC"). The SCAC re-alleges that claim for invasion of privacy by intrusion upon seclusion, with a material (and fatal) change, and attempts to revive a dismissed conversion claim against Twitter.

The SCAC fares even worse than the prior complaint because Plaintiffs have withdrawn the only factual allegation that conceivably supported their theory of liability – misuse of their data. It is uncontested that *Plaintiffs gave permission to Twitter to view and use their address books to match them and their friends*, and Plaintiffs no longer allege – because they cannot – that Twitter used that access for any other purpose. That Twitter allegedly copied Plaintiffs' contacts onto a computer server to facilitate consented-to matching of Plaintiffs with their friends does not meet the law's requirements for an intrusion claim.

Like its four predecessor complaints, the SCAC attempts to lump Twitter together with 14 other mobile application developers (collectively the "App Defendants"). However, the facts are distinct as to Twitter. Plaintiffs admit that Twitter informed them that Twitter's optional "Find Your Friends" feature would scan their mobile address books, and they agreed to this. In the SCAC, Plaintiffs merely take issue with Twitter's "upload" of their contacts, which they contend is an intrusion or conversion because it is not the same as "scanning" their contacts.

[1] Plaintiffs Beuershausen, Biondi, Dean, Dennis-Cooley, Green, Hodgins, Hoffman, King, Mandaywala, Moses, Paul, Sandiford, and Varner are collectively referred to herein as "Plaintiffs."

The problem with all this is that copying onto computer servers of contacts to which Twitter has been given access, for a purpose agreed to by Plaintiffs, is *not* a wrongful "intrusion." The tort of intrusion into seclusion provides a remedy for nonconsensual entry into a protected sphere of privacy. Here, Plaintiffs *invited* Twitter to access their data, and there is no allegation that Twitter engaged in any fraud or subterfuge. Copying, retention, and use of data do not fall within the scope of the intrusion tort, especially where, as here, Plaintiffs do not allege that Twitter did anything with the data when it obtained access other than perform the act (matching Twitter users) that the Plaintiffs approved.

Further, Twitter's alleged copying of data onto computer servers that Twitter accessed pursuant to express consent is not "highly offensive" conduct as a matter of law. What allegedly occurred here is nothing close to the type of behavior that the law considers sufficiently outrageous to support an intrusion claim. California appellate courts consider highly offensive conduct to include such horrific acts as videotaping for a television show a dying man and a severely injured, distraught, incoherent woman as they were being treated by emergency personnel, or obtaining access to someone's home under false pretense in order to make surreptitious recordings. Plaintiffs' mere contention that they did not expect Twitter to copy their contacts in order to match them with friends is not reasonable, and this belief, even if true, falls far short of the law's difficult standard for establishing that conduct was "highly offensive."

Plaintiffs' conversion claim fails on standing grounds, as this Court previously ruled, and fails on the merits as well. Plaintiffs consented to Twitter's access to the data, and Twitter did not interfere with any exclusive rights to possession. Plaintiffs do not allege a legally recognized, exclusive property interest in their address books.

Plaintiffs have had ample opportunity to fix the deficiencies in their pleadings. They have not done so in the SCAC, and they cannot do so in a future pleading. Accordingly, the SCAC must be dismissed in its entirety as to Twitter without further leave to amend.

II. ISSUES TO BE DECIDED

1. Whether Plaintiffs have sufficiently stated a claim in the SCAC upon which relief

may be granted for invasion of privacy by intrusion upon seclusion.

2. Whether Plaintiffs have alleged an "injury-in-fact" sufficient to satisfy the case or controversy requirement for standing to bring a conversion claim under Article III of the U.S. Constitution.

3. Whether Plaintiffs have sufficiently stated a claim in the SCAC upon which relief may be granted for conversion.

III. FACTUAL BACKGROUND

Twitter provides a service that allows users to communicate via the exchange of short messages known as "Tweets." Twitter users can find information they are interested in by "following" the Tweets of other users. One way for users to find accounts to "follow" is the "Follow Your Friends" feature, an optional feature in which Twitter uploads phone numbers from a user's mobile address book, compares those phone numbers with those of existing Twitter users, and displays any matching results. The "Follow Your Friends" feature is opt-in: Twitter users can skip it entirely.

The procedures for signing up for Twitter and using the "Follow Your Friends" feature are different from those used by the other App Defendants. Before a Twitter user can create an account and use the "Follow Your Friends" feature, that user must first accept Twitter's terms of service and privacy policy (collectively, "Terms"). (*See* Declaration of Sung Hu Kim ("Kim Decl."), ¶¶ 2-4, Exs. A, B, filed concurrently herewith.)[2] The Terms inform users that they may share, and Twitter may collect, information from "your address book so that we can help you find Twitter users you know." (*Id.* ¶¶ 9, 11, Exs. D-I, K-P.)

[2] The Court can consider documents on a motion to dismiss even if "not explicitly refer[red] to" but "the complaint necessarily relies upon." *Coto Settlement v. Eisenberg*, 593 F.3d 1031, 1038 (9th Cir. 2010); *see also Keithly v. Intelius Inc.*, 764 F. Supp. 2d 1257, 1262 (W.D. Wash. 2011). This "prevent[s] plaintiffs from surviving a Rule 12(b)(6) motion by deliberately omitting . . . documents upon which their claims are based." *Swartz v. KPMG LLP*, 476 F.3d 756, 763 (9th Cir. 2007) (internal quotation marks and citations omitted). Here, Twitter's terms of service and privacy policy are central to Plaintiffs' claims against Twitter. Plaintiffs omitted these and other related documents to avoid dismissal. Therefore, the Court should consider them in ruling on Twitter's Motion to Dismiss. *See id.*

Plaintiffs have had difficulty stating any claim against Twitter. On May 14, 2014, the Court issued its Order Granting in Part and Denying in Part Defendants' Motions to Dismiss Plaintiffs' CAC, dismissing thirteen of Plaintiffs' fourteen claims against Twitter and the other App Defendants, leaving only Plaintiffs' invasion of privacy claim standing. *Opperman v. Path, Inc.*, No. 13-cv-00453-JST, 2014 WL 1973378, at *33 (N.D. Cal. May 14, 2014). Plaintiffs' latest attempt, the SCAC, includes claims for invasion of privacy and conversion against Twitter and the other App Defendants.

Plaintiffs' 80-page SCAC includes just four paragraphs of allegations against Twitter. Plaintiffs allege that they signed up for Twitter and were presented with the option to use the "Follow Your Friends" feature. (SCAC ¶ 124.) Plaintiffs admit that Twitter informed them that it would "scan [their] contacts for people [they] already know on Twitter" if they opted to use the feature. (*Id.*) Plaintiffs nonetheless conclude that "[w]ithout prior user consent, the Twitter App uploaded iDevice address book data to Twitter" and, consequently, "Twitter improperly obtained the address book data belonging to Plaintiffs and class members." (*Id.* at ¶ 123.) As in prior complaints, Plaintiffs persist in failing to acknowledge their acceptance of the Terms in the SCAC, even though the Twitter application does not function unless a user accepts the Terms during the sign-up process. (Kim Decl. ¶¶ 2-5.)

Plaintiffs broadly allege as to all App Defendants that Plaintiffs purchased their mobile devices "with the expectation that address book data stored [thereon] would be secure, and could not be accessed or copied by third parties, including through Apps, without [their] express consent," and that had "[Plaintiffs] known that [their] address book data stored [thereon] was not secure, and could be accessed or copied by third parties, including through Apps, without [their] express consent, then [they] would not have paid as much for [their mobile devices]." (SCAC ¶¶ 141-42, 147-48, 153-54, 160-61, 167-68, 173-74, 179-80, 185-86, 191-92, 196-97, 202-03, 209-10, 215-16, 222-23, 229-30.) They also make the conclusory and unsupported claim that the App Defendants used, benefited, and profited from their address book data, injuring Plaintiffs by depriving them of the alleged "benefits and profits" of that use. (*Id.* ¶ 264.)

Equally important is what the SCAC omits. The Court chose not to dismiss Plaintiffs' intrusion claim as stated in the prior complaint, the CAC, because Plaintiffs had alleged that the App Defendants, including Twitter, misappropriated and used the contacts for their own benefit. *Opperman*, 2014 WL 1973378 at *26-27. As to Twitter, Plaintiffs alleged in the CAC that Twitter "used, stored, and kept [Plaintiffs' mobile address book] for eighteen months or so (likely in unsecure plain text)." (CAC ¶ 358.) *These allegations are deleted from the SCAC.* (*See* Attachments 1 & 2 (relevant excerpts from CAC and SCAC).)

IV. LEGAL STANDARDS

Federal Rule of Civil Procedure 12(b)(6) requires dismissal of a complaint if it fails to state a claim upon which relief can be granted.[3] Fed. R. Civ. P. 12(b)(6). To survive a motion to dismiss under Rule 12(b)(6), a complaint must allege "enough facts to state a claim to relief that is plausible on its face." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007). The Court does not accept as true "allegations that are merely conclusory, unwarranted, deductions of fact, or unreasonable inferences." *St. Clare v. Gilead Scis., Inc.*, 536 F.3d 1049, 1055 (9th Cir. 2008).

V. ARGUMENT

A. Plaintiffs Cannot State an Intrusion Upon Seclusion Claim Against Twitter.

To state a claim for intrusion upon seclusion, Plaintiffs must allege that Twitter: (a) intruded into a private place, conversation or matter; (b) in a manner highly offensive to a reasonable person. *Shulman v. Group W Prods., Inc.*, 18 Cal. 4th 200, 231 (1998). These "threshold elements" are intended to "screen out claims that do not involve a significant intrusion on a privacy interest." *Loder v. City of Glendale*, 14 Cal. 4th 846, 893 (1997). As set forth below, Plaintiffs fail to meet either prong, and their intrusion claim must be dismissed.

[3] There is no question that Twitter is entitled to move to dismiss all claims against it in the SCAC. *See, e.g., Bruton v. Gerber Products Co.*, No. 12–CV–02412–LHK, 2014 WL 172111, at *7 n.2 (N.D. Cal. Jan. 15, 2014) ("a defendant may challenge an amended complaint in its entirety"); *accord In re Sony Grand Wega KDF–E A10/A20 Series Rear Projection HDTV Television Litig.*, 758 F. Supp. 2d 1077, 1098 (S.D. Cal. 2010).

1. The Alleged Act of Uploading Contacts to Which Twitter was Given Access by Plaintiffs Was Not an "Intrusion."

Plaintiffs' intrusion claim fails because there has been no "intrusion" upon their address book contacts. The tort of intrusion encompasses "unconsented-to physical intrusion into the home, hospital room or other place the privacy of which is legally recognized, as well as unwarranted sensory intrusions such as eavesdropping, wiretapping, and visual or photographic spying." *Shulman*, 18 Cal. 4th at 230-31. "To prove actionable intrusion, the plaintiff must show the defendant *penetrated some zone of physical or sensory privacy* surrounding, or obtained *unwanted access* to data about, the plaintiff." *Id.* at 232 (emphasis added). The plaintiff "must show (a) an actual, subjective expectation of seclusion or solitude in the place, conversation, or matter, and (b) that the expectation was objectively reasonable." *Med. Lab. Mgmt. Consultants v. Am. Broad. Cos.*, 306 F.3d 806, 812-13 (9th Cir. 2002).

Put simply, "intrusion" is the act of invading a person's "protected sphere of privacy." *Pearson v. Dodd*, 410 F.2d 701, 704 (D.C. Cir. 1969). It is not improper *use* of information, and it cannot possibly occur where the defendant has been invited into the "place, conversation, or matter." *See id.* at 705-06 (distinguishing intrusion injury from publication injury); *Med. Lab. Mgmt.*, 306 F.3d at 818 (rejecting intrusion claim based on surreptitious tape recording where plaintiff freely shared information with undercover reporters). If *access* to data is given to the defendant, there can be no intrusion claim, and an intrusion claim does not arise for the distinct acts of retention, copying, transfer or use of the data *afterward*.[4] *See* Restatement (Second) Torts (1977), § 672B, cmt. a (intrusion upon seclusion tort "consists solely of an intentional interference with [plaintiff's] interest in solitude or seclusion").

[4] Even if the Court takes a broader view and determines that Plaintiffs can properly state an intrusion claim by alleging actions subsequent to the intrusion itself (e.g., post-intrusion "copying"), Plaintiffs' claim still fails. Plaintiffs have not alleged any harm or particularized injury resulting from Twitter's alleged actions after accessing Plaintiffs' contacts to support Article III standing. *See Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 180-81 (2000) (Article III standing requires "concrete and particularized" injury).

To illustrate, in *Marich v. MGM/UA Telecommunications*, the plaintiffs sued the producers and distributors of a television show for, *inter alia*, intrusion upon seclusion for broadcasting a recorded telephone conversation of the police informing the plaintiffs of their son's death. 113 Cal. App. 4th 415, 419-20 (2003). Apart from their intrusion claim for the act of recording, the plaintiffs maintained that the editing of the videotape to enhance the sound of their voices constituted a separate intrusion upon their seclusion. *Id.* at 430. The court rejected the plaintiffs' claim on the grounds that the act of enhancing the video, even if "highly offensive," was not an act that intruded on any zone of privacy. *Id.* at 431. "What a defendant does with a surreptitious recording after obtaining it may affect the measure of damages[,]" the court explained, "but it is not a new 'obtaining.'" *Id.* at 432.

Here, as in *Marich*, Plaintiffs' intrusion upon seclusion claim fails because Plaintiffs object not to Twitter's access to their address book information, but to Twitter's uploading of their information after that access. (*See, e.g.*, SCAC ¶¶ 123 (alleging that, without prior consent, "the Twitter App uploaded iDevice address book data to Twitter or someone acting on its behalf"), 246 (alleging an intrusion due to the App Defendants' "surreptitiously obtaining, improperly gaining knowledge, reviewing and retaining Plaintiffs' private address books").) It is beyond dispute that Plaintiffs *wanted* Twitter to access their data. Plaintiffs affirmatively requested that Twitter scan their contacts in order to use the optional "Follow Your Friends" feature. (CAC ¶¶ 355-58; SCAC ¶ 125.) Copying data that has been made accessible onto computer servers does not invade a person's sphere of privacy, and it is not intrusion upon seclusion.

2. Plaintiffs' Consent Forecloses Any Reasonable Privacy Expectation in their Address Books As to Twitter.

By agreeing to have their contacts scanned by Twitter, Plaintiffs no longer had a reasonable expectation that those contacts would be private as to Twitter and unavailable for the matching service that Twitter offered to Plaintiffs.[5] "The tort is proven only if the plaintiff had an

[5] By this Motion, Twitter is not raising the issue of whether Plaintiffs' contacts are "private" under California law. Rather, Plaintiffs entered into an agreement with Twitter under which they

objectively reasonable expectation of seclusion or solitude in the place, conversation or data source." *See Shulman*, 18 Cal. 4th at 232. A plaintiff has no reasonable expectation of privacy where he or she actually consents to the behavior or invites the "intrusion." *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 26 (1994); *see also Cramer v. Consolidated Freightways, Inc.*, 209 F.3d 1122, 1130 (9th Cir. 2000) (recognizing consent as a defense to a privacy action); *see also* Cal. Civ. Code § 3515 ("He who consents to an act is not wronged by it").

Plaintiffs consented to Twitter's access by inviting Twitter to "scan" their mobile address books. (*See* CAC ¶ 357; SCAC ¶ 124; Kim Decl., ¶¶ 2-4, 9, 11, Exs. A-B, D-I, K-P.) Plaintiffs nowhere allege in the SCAC, the current complaint, that Twitter accessed Plaintiffs' information for purposes other than, or in a manner inconsistent with, carrying out the disclosed and consented-to task of determining whether Plaintiffs' acquaintances were using Twitter. (*Cf.* CAC ¶ 358 (alleging that Twitter "used, stored, and kept [Plaintiffs' mobile address book] for eighteen months or so (likely in unsecure plain text)" (deleted from the SCAC); *Opperman*, 2014 WL 1973378 at *26 (holding, in the context of the CAC, that consent to scan may be invalid if the consent language does not disclose that "the app would transmit a copy of the address book to Defendants *for their own use*" (emphasis added)).)

Nor do Plaintiffs allege that Twitter, in obtaining access to their address books, disclosed their contact data to the public at large, used it for purposes other than those disclosed and approved by Plaintiffs, or committed fraud on Plaintiffs. *Compare Dietemann v. Time, Inc.*, 449 F.2d 245 (9th Cir. 1971) (plaintiff's invitation of undercover reporter into his home based on a ruse did not constitute consent to broad disclosure of intimate facts to the public), *with Med. Lab. Mgmt.*, 306 F.3d at 312-19 (plaintiff's willingness to give tour of lab, give access to administrative offices, and engage in a long discussion of plaintiff's business with reporters established no reasonable expectation of privacy).

In a thoughtful decision issued last week, Judge Koh found that consent to the "scanning" of emails by Yahoo necessarily included consent to storage of emails, and no claim could be

---

gave Twitter access to those contacts.

made based on the handling of data consistent with a user's consent. *In re Yahoo Mail Litig.*, 5:13-cv-04980, 2014 WL 3962824, at *9 (N.D. Cal. Aug. 12, 2014) ("*Yahoo Mail*"). The *Yahoo Mail* plaintiffs asserted that even if they agreed in terms of service that Yahoo could "scan or analyze" their emails, Yahoo violated the Wiretap Act by collecting and storing them. *Id.*

Judge Koh rejected the plaintiffs' claim, even though the acts of collecting and storing were not expressly disclosed in Yahoo's terms, because

> the reasonable user would know that the language that Yahoo 'scan[s] and analyze[s]' email content necessarily means Yahoo simultaneously collects and stores the email content, *i.e.*, the reasonable user would know that 'scanning and analyzing' requires Yahoo to collect and store the email content. *In other words, the Court finds it implausible that users did not – after agreeing, based on the [terms], to Yahoo's scanning and analysis of emails – realize that in order to engage in analysis of emails, Yahoo would have to store the emails somewhere on its servers.*

Id. (emphasis added).

Similarly here, Plaintiffs gave consent to Twitter's accessing their contacts, so they could not have retained a reasonable expectation of privacy for their contacts as to Twitter. Uploading a copy of those contacts fell within the scope of that consent, and Plaintiffs have no intrusion claim based on the "Follow Your Friends" feature.

3. Twitter's Actions Were Not "Highly Offensive."

Even if we assume that Plaintiffs have alleged an act of "intrusion," Twitter's actions were not "highly offensive," *i.e.*, an "egregious breach of ... social norms." *Hill*, 7 Cal. 4th at 37. Courts are required to make a threshold determination of offensiveness and may adjudicate the issue as a matter of law. *Miller v. Nat'l Broad. Co.*, 187 Cal. App. 3d 1463, 1483 (1986) ("there is a preliminary determination of 'offensiveness' which must be made by the court in discerning the existence of a cause of action for intrusion"); *Hill*, 7 Cal. 4th at 40 ("If the undisputed material facts show no reasonable expectation of privacy or an insubstantial impact on privacy interests, the question of invasion may be adjudicated as a matter of law").

This Court previously held that the question of whether the "theft" of Plaintiffs' address book information was "highly offensive" was best left to a jury. *Opperman*, 2014 WL 1973378

at *27. But the SCAC contains no allegations that *Twitter* uploaded the address book information and retained it for its own use. Plaintiffs have not alleged that Twitter stole anything or did anything other than match Plaintiffs with their friends using Twitter. At most, Plaintiffs have alleged that they did not realize that it was necessary for Twitter to copy their contacts onto computer servers in order to accomplish the agreed-to task.

These allegations rise nowhere near the "egregious breach of the social norms" necessary for a finding of "highly offensive" intrusion. *See Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 295 (2009); *Hill*, 7 Cal. 4th at 37; *Miller*, 187 Cal. App. 3d at 1483, n.6. Twitter did not secretly record or spy on Plaintiffs, let alone in a traumatic private circumstance. *Shulman*, 18 Cal. 4th 200 (videotaping accident victim en route to hospital); *Miller*, 187 Cal. App. 3d 1463 (videotaping dying man during cardiac arrest while in his own home). Nor did Twitter invade Plaintiffs' bodily privacy. *Sheehan v. San Francisco 49ers, Ltd.*, 45 Cal. 4th 992 (2009) (security search during football game that plaintiffs alleged was akin to groping); *Hill*, 7 Cal. 4th 1 (monitoring student athletes during urine test). Twitter did not lie about its identity or purpose in order to gain access to Plaintiffs' private home or to obtain private information. *Taus v. Loftus*, 40 Cal 4th 683 (2007) (investigator posing as mental health associate); *Sanchez-Scott v. Alza Pharmaceuticals*, 86 Cal. App. 4th 365 (2001) (sales associate participating in patient's breast exam, while being introduced only as someone observing the doctor's work).

The California Supreme Court made clear in *Hernandez* that the "highly offensive" element of the intrusion into seclusion tort required consideration of the alleged intruder's "motives and objectives." 47 Cal. 4th at 295. "[N]o cause of action will lie for accidental, misguided, or excusable acts of overstepping upon legitimate privacy rights." *Id.* Similarly, in *Sheehan*, the state Supreme Court said, "If voluntary consent is present, a defendant's conduct will rarely be deemed 'highly offensive to a reasonable person' so as to justify tort liability." 45 Cal. 4th at 1000. Here, Twitter obtained access to Plaintiffs' mobile address books through consent, and the allegation that Twitter overstepped merely by uploading that information falls far short of an act that is "highly offensive."

Thus, Twitter's actions cannot be "highly offensive" as a matter of law.

4. Twitter's Actions Were Necessary to Provide the Service.

The *Hernandez* decision confirmed that a court must consider, in determining whether an intrusion is sufficiently serious to give rise to a tort, "all of the surrounding circumstances, including the 'degree and setting' of the intrusion and 'the intruder's 'motives and objectives.'" *Id*. (quoting *Shulman*, 18 Cal. 4th at 200); *see also Cramer*, 209 F.3d at 1131 ("privacy rights can be altered or waived under California law and must be considered in context").

In *Hernandez*, the California Supreme Court found that the defendant had sufficient justification to videotape plaintiffs' offices. 47 Cal. 4th at 296-97. The court made clear that the case did "not involve surveillance measures conducted for *socially repugnant or unprotected reasons*," such as harassment, blackmail, or prurient curiosity. *Id.* at 297 (emphasis added). Rather, the undisputed evidence showed "that defendants installed video surveillance equipment in plaintiffs' office, and activated it three times after they left work, in order to confirm a strong suspicion—triggered by publicized network tracking measures—that an unknown staff person was engaged in unauthorized and inappropriate computer use at night." *Id.*

Here, Twitter simply took steps to provide a service that Plaintiffs requested, using the technology available to it. Plaintiffs take issue with the "uploading" of the address book data, but, again, they do not allege any plausible way for Twitter to "scan" their contacts *other* than by comparing those contacts with user data on Twitter's own computer servers. *See Yahoo Mail*, 2014 WL 3962824 at *9. In any event, even if "scan" were found to exclude the act of storing data on Twitter servers, that storage cannot possibly be "socially repugnant" and unjustified, given that Plaintiffs voluntarily provided access to the data and asked Twitter to use it to find their friends and there is no contention that Twitter used it for any other purpose than to provide the service Plaintiffs requested.

B. Plaintiffs Also Cannot State a Conversion Claim Against Twitter.

1. Lacking Standing, Plaintiffs Are Unable to Resurrect Their Failed Conversion Claim.

The Court has already determined that Plaintiffs lack standing to bring a conversion claim, and the SCAC alleges nothing to change this result. *Opperman*, 2014 WL 1973378 at *23. Article III standing requires Plaintiffs to sufficiently allege: (1) an injury-in fact; (2) causation; and (3) redressability. *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992). To allege an injury-in-fact, Plaintiffs must show "an invasion of a legally protected interest which is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical." *Id.*

As in the CAC, Plaintiffs' allegations in the SCAC that Twitter accessed and copied their address books are insufficient to establish an injury in fact. *Opperman*, 2014 WL 1973378 at *23 n.22 ("copying [electronically stored private information] without any meaningful economic injury to consumers is insufficient to establish standing" on the basis of property rights"). Indeed, as the Court already noted in its previous Order, "'[i]n cases where the alleged converter has only a copy of the owner's property and the owner still possesses the property itself, the owner is in no way being deprived of the use of his property.'" *Id.* (quoting *FMC Corp. v. Capital Cities/ABC, Inc.*, 915 F.2d 300, 303-04 (7th Cir. 1990)).

Similarly insufficient are Plaintiffs' conclusory allegations that by uploading their address books, Twitter deprived them of "benefits and profits" and, in turn, benefited itself. (*See* SCAC ¶¶ 125, 264.) Plaintiffs "must do more than point to the dollars in a defendant's pocket; [they] must sufficiently allege that in the process [they] lost dollars of [their] own." *Yunker v. Pandora Media, Inc.*, No. 11-cv-03113-JSW, 2013 WL 1282980 (N.D. Cal. Mar. 26, 2013). The SCAC is bereft of any such plausible allegations. *In re Google Android Consumer Privacy Litig.*, No. 11-md-02264-JSW, 2013 WL 1283236, at *4 (N.D. Cal. Mar. 26, 2013) (dismissing complaint against Google for lack of standing, noting that the plaintiffs "do not allege they attempted to sell their personal information, that they would do so in the future, or that they were foreclosed from entering into a value for value transaction relating to their PII, as a result of the Google

Defendants' conduct"). For these reasons alone, Plaintiffs' conversion claim must be dismissed.

2. Plaintiffs Cannot Allege Any Elements Of Their Conversion Claim.

Plaintiffs' conversion claim fails on the merits as well. "A conversion occurs where the defendant wrongfully exercises dominion over the property of another." *Bank of New York v. Fremont Gen. Corp.*, 523 F.3d 902, 914 (9th Cir. 2008). To state a conversion claim, a plaintiff must show "ownership or right to possession of property, wrongful disposition of the property right and damages." *Kremen v. Cohen*, 337 F.3d 1024, 1029 (9th Cir. 2003) (quoting *G.S. Rasmussen & Assocs., Inc. v. Kalitta Flying Serv., Inc.*, 958 F.2d 896, 906 (9th Cir. 1992)). Plaintiffs must also "prove that it did not consent to the defendant's exercise of dominion." *Bank of New York*, 523 F.3d at 914.

a) Twitter Did Not Exercise Dominion Over Plaintiffs' Data.

Plaintiffs cannot show that Twitter wrongfully exercised dominion over their data. First, as discussed above, Plaintiffs gave Twitter access to Plaintiffs' contacts for the purpose of determining if any of their acquaintances were also using Twitter. (SCAC, ¶¶ 124, 259.) Plaintiffs' consent to Twitter's actions vitiates their conversion claim. *See Bank of New York*, 523 F. 3d at 914 ("The law is well settled that there can be no conversion where an owner either expressly or impliedly assents to or ratifies the taking, use or disposition of his property") (quotation omitted); *see also Yahoo Mail*, 2014 WL 3962824 at *9 (holding that by obtaining consent to scan emails, Yahoo necessarily obtained consent to collect and store those emails).

Second, Plaintiffs still have their contacts in their possession. *See FMC Corp.*, 915 F.2d at 303-04 (no claim for conversion where the defendant only has "a copy of the owner's property"); *accord Pearson v. Dodd*, 410 F.2d 701, 706-07 (D.C. Cir. 1969). Plaintiffs do not allege any facts showing that Twitter "assum[ed] control or ownership over" the address book information, applied that information to its own use, or did anything at all with the address book information other than provide Plaintiffs with the service they requested. *Hartford Financial Corp. v. Burns*, 96 Cal. App. 3d 591, 598 (1979).

b) Plaintiffs Lack A Sufficient Intangible Property Interest.

Furthermore, where, as here, a conversion claim is based on intangible rather than tangible property, a plaintiff must have a sufficient interest in the intangible property to support a conversion claim. *Kremen*, 337 F.3d at 1030. Courts apply a three-part test to make this determination: (1) "there must be an interest capable of precise definition," (2) "it must be capable of exclusive possession or control," and (3) "the putative owner must have established a legitimate claim to exclusivity." *Id.*

Plaintiffs do not have a sufficient intangible property interest in their address book information. Unlike in *Kremen*, where the plaintiff was deprived of his exclusive right to a registered domain name, Plaintiffs' address books lack well-defined characteristics necessary to support a conversion claim. Plaintiffs do not plausibly allege that their address books were composed of data for which they had exclusive rights, or were valued, bought and sold for any amount.

Rather, Plaintiffs' address book information consists of information about *other people*, much or all of which is nonconfidential and even collected automatically by mobile devices. This type of information cannot support a conversion claim. *See Olschewski v. Hudson*, 87 Cal. App. 282, 286-88 (1927) (holding that the plaintiff lacked a sufficient property interest in a customer list to support a conversion claim). Thus, Plaintiffs have failed to state a claim for conversion.

C. Plaintiffs Should be Denied Leave To Amend.

A district court "may in its discretion deny leave to amend 'due to . . . repeated failure to cure deficiencies by amendments previously allowed, . . . [and] futility of amendment.'" *Zucco Partners, LLC v. Digimarc Corp.*, 552 F.3d 981, 1007 (9th Cir. 2009) (quoting *Leadsinger, Inc. v. BMG Music Publ'g*, 512 F.3d 522, 532 (9th Cir. 2008)); *see also Destfino v. Reiswig*, 630 F.3d 952, 959 (9th Cir. 2011) ("It is well-established that a court may dismiss an entire complaint with prejudice where plaintiffs have failed to plead properly after 'repeated opportunities'") (*quoting Neubronner v. Milken*, 6 F.3d 666, 672 (9th Cir. 1993)).

Over the course of two and a half years, Plaintiffs have been given five opportunities to

plead viable claims against Twitter. Plaintiffs have fallen short, and this Court and Twitter should not be further burdened with this lawsuit. Further amendment would be futile, and Plaintiffs' claims against Twitter should be dismissed in their entirety and without leave to amend.

VI. CONCLUSION

For the reasons stated above, Twitter respectfully requests that the Court dismiss all claims against Twitter in the Second Consolidated Amended Complaint, with prejudice.

DATED: August 21, 2014

PERKINS COIE LLP

By: */s/ Timothy L. Alger*
Timothy L. Alger

Attorneys for Defendant
Twitter, Inc.

ATTACHMENT 1

349. Plaintiffs Biondi, Hodgins, Hoffman, Mandaywala, Paul, and Sandiford, each recall navigating to various screens on and using the Yelp! App. They recall providing a log in and navigating within the Yelp! App to a screen containing a ["Find Friends"] button with the accompanying displayed text:

> "Find friends on Yelp using your Contacts and Facebook friends? You'll be able to see their bookmarks and find out when they're nearby. [Yes, Find Friends] [No, Skip This]",

and pressing the ["Yes, Find Friends"] button. Plaintiffs do not recall being presented at any time in that process with an intervening alert or pop-up display indicating that the *Yelp!* App would transfer any portion of his or her private mobile address book to Yelp to perform this function or warning that such a transmission was about to occur.

350. The displayed Yelp! App text does not request permission to upload any address book materials from Plaintiffs' iDevices or externally transmit any of Plaintiffs' mobile address book material.

351. Published reports indicate that before February 2012 when an iDevice Yelp! App user tapped the ["Yes, Find Friends"] button, the iDevice would automatically, without first asking for or securing consent to do so, initiate a call, copy bulk portions of the user's address book, and the iDevice would then relay, upload and transmit those materials via Wi-Fi, 3G and the Internet to Yelp's servers, where Yelp then at its discretion remotely stored, used and kept the materials. This occurred to the identified Plaintiffs multiple times.

352. Yelp thus obtained, retained, disclosed and de-privatized these Plaintiffs' valuable private address books and used their iDevices without seeking (or obtaining) authorization to do so. Yelp and its App never asked Plaintiffs if they could do any of these things.

353. Following adverse media reports, Yelp modified its App in mid-February 2012 with a new halt and an alert that appeared when a user tapped the ["Find Friends"] button that reads:

> "**Find Friends** To find friends, we'll need to upload your contacts to Yelp. Don't worry, we're not storing them. [No Thanks] [OK]"

Twitter

354. App Defendant Twitter built the Twitter App using Apple-supplied components and tools, with Apple providing substantial assistance through the Program and a digital certificate for the App to function on iDevices. Following Apple's review (during which time Apple learned or should have learned of the App's malicious, prohibited features), Apple released, promoted and deployed the Twitter App on the App Store and served as Twitter's world-wide agent for the solicitation of orders for and the delivery of the App to iDevice end-users.

355. Plaintiffs Beuershasen, Biondi, Dean, Dennis-Cooley, Green, Hodgins, Hoffman, King, Mandaywala, Moses, Paul and Varner (the "Twitter Plaintiffs") recall opening the Twitter App, signing up via its displayed registration screen, and using the App. They were initially presented a "Welcome" screen prompting them to press an on-screen button labeled ["Follow your friends"], under which was written in small type: "Scan your contacts for people you already know on Twitter." They also recall another screen labeled "Follow Friends" that similarly prompted them to press an on-screen button labeled ["Follow your friends"], under which was written in small type the identical phrase as before.

356. The App's ["Follow your friends"] button-bar and accompanying textual phrase do not request for permission to upload or transmit elsewhere any of the Plaintiffs' iDevice address book materials.

357. As prompted, prior to February 2012, each Plaintiff pressed the displayed ["Follow your friends"] button-bar. Plaintiffs recall no alerts or warnings that their private mobile address books were being taken.

358. According to Twitter, when Twitter App users tapped the ["Follow your friends"] button-bar prior to February 2012, the App connected their iDevice to Twitter's servers uploaded all email addresses and phone numbers in the iDevice owner's mobile address book, which Twitter used, stored and kept for eighteen months or so (likely in unsecure plain text). This occurred to the identified Plaintiffs.

359. After media questioned the Twitter App's privacy practices and secret address book collection function, sometime after February 6, 2012 Twitter modified the language on its Twitter

App's "Find Friends" screen and ["Follow your friends"] button, replacing the phrase "scan your contacts" with the phrase "upload your contacts" (thus essentially conceding the non-equivalence of those words) and also added the following intervening alert:

> "**Find Friends on Twitter** We will securely upload your contacts to help you find friends and suggest users to follow on Twitter. [Cancel] [OK]"

Foodspotting

360. App Defendant Foodspotting built the Foodspotting App using Apple-supplied components and tools, with Apple providing substantial assistance through the Program and a digital certificate for the App to function on iDevices. Following Apple's review (during which time Apple learned or should have learned of the App's malicious, prohibited features), Apple released, promoted and deployed the Foodspotting App on the App Store and served as Foodspotting's world-wide agent for the solicitation of orders for and the delivery of the App to iDevice end-users.

361. Plaintiffs King and Sandiford (the "Foodspotting Plaintiffs") recall opening the Foodspotting App, signing up via its registration screen, and using the App. More particularly, they recall navigating to the Foodspotting App's "Follow People" screen containing an on-screen button labeled ["Find iPhone Contacts."]. While on that screen, the Foodspotting Plaintiffs tapped that button. The screen contained no warnings whatsoever indicating that the App was relaying his or her mobile address book to Foodspotting.

362. The displayed button and screen menu name do not constitute a request for permission or transmit or upload Plaintiffs' iDevices address book materials and Plaintiffs did not consent to this.

363. According to defendant Foodspotting's February 15, 2012 company blog, when App users tapped the ["Find iPhone Contacts]" button, the iDevice would, silently and without first asking or securing consent, initiate an Internet call, copy bulk portions of the user's address book (in particular, all email addresses), and the iDevice would then relay and transmit those materials via Wi-Fi, 3G and the Internet to Foodspotting's servers, where Foodspotting then remotely used and stored the materials. Upon information and belief, this occurred to the Foodspotting Plaintiffs

ATTACHMENT 2

served as Yelp's world-wide agent for the solicitation of orders for and the delivery of the App to iDevice end-users.

119. Without prior user consent, the Yelp! App uploaded iDevice address book data to Yelp or someone acting on its behalf. As a consequence, Yelp improperly obtained the address book data belonging to Plaintiffs and class members.

120. Plaintiffs Biondi, Hodgins, Hoffman, Mandaywala, and Paul (the "Yelp Plaintiffs") each recall navigating to various screens on and using the Yelp! App. They recall providing a log in and navigating within the Yelp! App to a screen containing a ["Find Friends"] button with the accompanying displayed text: "Find friends on Yelp using your Contacts and Facebook friends? You'll be able to see their bookmarks and find out when they're nearby. [Yes, Find Friends] [No, Skip This]", and pressing the ["Yes, Find Friends"] button. Plaintiffs do not recall being presented at any time in that process with an intervening alert or pop-up display indicating that the Yelp! App would transfer any portion of his or her private address book to Yelp to perform this function or warning that such a transmission was about to occur.

121. Yelp benefitted substantially from its misappropriation of users' address books. On information and belief, the misappropriation of that property enabled the company to more rapidly grow its user base, avoid the costs of customer acquisition, enhance its social networking features, and increase the value of the company, among other benefits.

Twitter

122. App Defendant Twitter built the Twitter App using Apple-supplied components and tools, with Apple providing substantial assistance through the Program. Following Apple's review (during which time Apple learned or should have learned of the App's malicious, prohibited features), Apple released, promoted and deployed the Twitter App on the App Store and served as Twitter's world-wide agent for the solicitation of orders for and the delivery of the App to iDevice end-users.

123. Without prior user consent, the Twitter App uploaded iDevice address book data to Twitter or someone acting on its behalf. As a consequence, Twitter improperly obtained the address book data belonging to Plaintiffs and class members.

124. Plaintiffs Beuershausen, Biondi, Dean, Dennis-Cooley, Green, Hodgins, Hoffman, King, Mandaywala, Moses, Paul, Sandiford, and Varner (the "Twitter Plaintiffs") recall opening the Twitter App, signing up via its displayed registration screen, and using the App. They were initially presented a "Welcome" screen prompting them to press an on-screen button labeled ["Follow your friends"], under which was written in small type: "Scan your contacts for people you already know on Twitter." They also recall another screen labeled "Follow Friends" that similarly prompted them to press an on-screen button labeled ["Follow your friends"], under which was written in small type the identical phrase as before.

125. Twitter benefitted substantially from its misappropriation of users' address books. On information and belief, the misappropriation of that property enabled the company to more rapidly grow its user base, avoid the costs of customer acquisition, enhance its social networking features, and increase the value of the company, among other benefits.

Foodspotting

126. App Defendant Foodspotting built the Foodspotting App using Apple-supplied components and tools, with Apple providing substantial assistance through the Program. Following Apple's review (during which time Apple learned or should have learned of the App's malicious, prohibited features), Apple released, promoted and deployed the Foodspotting App on the App Store and served as Foodspotting's world-wide agent for the solicitation of orders for and the delivery of the App to iDevice end-users.

127. Without prior user consent, the Foodspotting App uploaded iDevice address book data to Foodspotting or someone acting on its behalf. As a consequence, Foodspotting improperly obtained the address book data belonging to Plaintiffs and class members.

128. Plaintiffs King and Sandiford (the "Foodspotting Plaintiffs") recall opening the Foodspotting App, signing up via its registration screen, and using the App. More particularly, they recall navigating to the Foodspotting App's "Follow People" screen containing an on-screen button labeled ["Find iPhone Contacts."]. While on that screen, the Foodspotting Plaintiffs tapped that button. The screen contained no warnings whatsoever indicating that the App was relaying his or her address book to Foodspotting.